



ABSTRACT OF THE DISCLOSURE

A system for securely using digital signatures in a commercial cryptographic system that allows industry-wide security policy and authorization information to be encoded into the signatures and certificates by employing attribute certificates to enforce policy and authorization requirements. Verification of policy and authorization requirements is enforced in the system by restricting access to public keys to users who have digitally signed and agreed to follow rules of the system. These rules can also ensure that payment is made for public and private key usage. Additionally, users can impose their own rules and policy requirements on transactions in the system.

09870584-112001